Terms used: **spoof email** Found **268** of **207,474**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Why spoofing is serious internet fraud
Tamara Dinev
October 2006 **Communications of the ACM**, Volume 49 Issue 10
Publisher: ACM Press
Full text available: pdf(1.17 MB) html(23.34 KB) Additional Information: full citation, abstract, references, index terms

Fake Web sites fool the unwary into divulging personal data, undermining all consumers' trust in e-commerce, no matter how trustworthy the authentic online business truly is.

2 Security, privacy & ethics: Designing ethical phishing experiments: a study of (ROT13) rOnl query features
Markus Jakobsson, Jacob Ratkiewicz
May 2006 **Proceedings of the 15th international conference on World Wide Web WWW '06**
Publisher: ACM Press
Full text available: pdf(389.53 KB) Additional Information: full citation, abstract, references, index terms

We study how to design experiments to measure the success rates of phishing attacks that are *ethical* and *accurate*, which are two requirements of contradictory forces. Namely, an *ethical* experiment must not expose the participants to any risk; it should be possible to locally verify by the participants or representatives thereof that this was the case. At the same time, an experiment is *accurate* if it is possible to argue why its success rate is not an upper or lower b ...

Keywords: accurate, ethical, experiment, phishing, security

3 Security: Protecting people from phishing: the design and evaluation of an embedded training email system
Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge
April 2007 **Proceedings of the SIGCHI conference on Human factors in computing systems CHI '07**
Publisher: ACM Press
Full text available: pdf(1.16 MB) Additional Information: full citation, abstract, references, index terms

Phishing attacks, in which criminals lure Internet users to websites that impersonate

legitimate sites, are occurring with increasing frequency and are causing considerable harm to victims. In this paper we describe the design and evaluation of an embedded training email system that teaches people about phishing during their normal use of email. We conducted lab experiments contrasting the effectiveness of standard security notices about phishing with two embedded training designs we develope ...

Keywords: email, embedded training, phishing, situated learning, usable privacy and security

4 Catching phish: Decision strategies and susceptibility to phishing

Julie S. Downs, Mandy B. Holbrook, Lorrie Faith Cranor

July 2006 **Proceedings of the second symposium on Usable privacy and security SOUPS '06**

Publisher: ACM Press

Full text available: pdf(266.61 KB) Additional Information: full citation, abstract, references, index terms

Phishing emails are semantic attacks that con people into divulging sensitive information using techniques to make the user believe that information is being requested by a legitimate source. In order to develop tools that will be effective in combating these schemes, we first must know how and why people fall for them. This study reports preliminary analysis of interviews with 20 non-expert computer users to reveal their strategies and understand their decisions when encountering possibly suspi ...

Keywords: mental models, phishing, qualitative methods

5 Passwords and phishing: Learning to detect phishing emails

Ian Fette, Norman Sadeh, Anthony Tomasic

May 2007 **Proceedings of the 16th international conference on World Wide Web WWW '07**

Publisher: ACM Press

Full text available: pdf(235.33 KB) Additional Information: full citation, abstract, references, index terms

Each month, more attacks are launched with the aim of making web users believe that they are communicating with a trusted entity for the purpose of stealing account information, logon credentials, and identity information in general. This attack method, commonly known as "phishing," is most commonly initiated by sending out emails with links to spoofed websites that harvest information. We present a method for detecting these attacks, which in its most general form is an application of machin ...

Keywords: email, filtering, learning, phishing, semantic attacks, spam

6 Authentication: Message authentication by integrity with public corroboration

P. C. van Oorschot

September 2005 **Proceedings of the 2005 workshop on New security paradigms NSPW '05**

Publisher: ACM Press

Full text available: pdf(2.31 MB) Additional Information: full citation, abstract, references, index terms

One of the best-known security paradigms is to use authentication as the basis for access control decisions. We turn this around, and instead rely on access control (or more precisely, integrity) as the basis for authentication. We propose a simple, practical means by which data origin assurances for message authentication are based on corroboration, for example by cross-checking with information made available by a known source or at a specified location (e.g., web page). The security re ...

Keywords: data origin authentication, digital signatures, email source authentication, message authentication, phishing, security by integrity, spam, undetected key compromise

7 PHONEY: Mimicking User Response to Detect Phishing Attacks
Madhusudhanan Chandrasekaran, Ramkumar Chinchani, Shambhu Upadhyaya
June 2006 **Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks WOWMOM '06**
Publisher: IEEE Computer Society
Full text available: pdf(348.62 KB) Additional Information: full citation, abstract, index terms

Phishing scams pose a serious threat to end-users and commercial institutions alike. Email continues to be the favorite vehicle to perpetrate such scams mainly due to its widespread use combined with the ability to easily spoof them. Several approaches, both generic and specialized, have been proposed to address this problem. However, phishing techniques, growing in ingenuity as well as sophistication, render these solutions weak. In this paper we propose a novel approach to detect phishing atta ...

8 Security: Why phishing works
Rachna Dhamija, J. D. Tygar, Marti Hearst
April 2006 **Proceedings of the SIGCHI conference on Human Factors in computing systems CHI '06**
Publisher: ACM Press
Full text available: pdf(1.33 MB) Additional Information: full citation, abstract, references, citings, index terms

To build systems shielding users from fraudulent (or phishing) websites, designers need to know which attack strategies work and why. This paper provides the first empirical evidence about which malicious strategies are successful at deceiving general users. We first analyzed a large set of captured phishing attacks and developed a set of hypotheses about why these strategies might work. We then assessed these hypotheses with a usability study in which 22 participants were shown 20 web sites and ...

Keywords: phishing, phishing user study, security usability, why phishing works

9 Envisioning communication: task-tailorable representations of communication in asynchronous work
Christine M. Neuwirth, James H. Morris, Susan Harkness Regli, Ravinder Chandhok, Geoffrey C. Wenger
November 1998 **Proceedings of the 1998 ACM conference on Computer supported cooperative work CSCW '98**
Publisher: ACM Press
Full text available: pdf(1.18 MB) Additional Information: full citation, references, citings, index terms

Keywords: asynchronous communication, awareness, collaborative work, electronic mail, external representations, incremental formalization, interfaces, visualization

10 Security: Do security toolbars actually prevent phishing attacks?
Min Wu, Robert C. Miller, Simson L. Garfinkel
April 2006 **Proceedings of the SIGCHI conference on Human Factors in computing systems CHI '06**

Publisher: ACM Press

Full text available: pdf(532.71 KB) Additional Information: full citation, abstract, references, citings, index terms

Security toolbars in a web browser show security-related information about a website to help users detect phishing attacks. Because the toolbars are designed for humans to use, they should be evaluated for usability -- that is, whether these toolbars really prevent users from being tricked into providing personal information. We conducted two user studies of three security toolbars and other browser security indicators and found them all ineffective at preventing phishing attacks. Even though su ...

Keywords: e-commerce, user interface design, user study, world wide web and hypermedia

11 Spam and the ongoing battle for the inbox

Joshua Goodman, Gordon V. Cormack, David Heckerman
February 2007 **Communications of the ACM**, Volume 50 Issue 2

Publisher: ACM Press

Full text available: pdf(1.30 MB) html(44.06 KB) Additional Information: full citation, abstract, references, index terms

Even as spammers and phishers try evermore sophisticated techniques to get past filters and into users' mailboxes, anti-spam researchers have managed to stay several steps ahead, so far.

12 Passwords and phishing: Cantina: a content-based approach to detecting phishing web sites

Yue Zhang, Jason I. Hong, Lorrie F. Cranor
May 2007 **Proceedings of the 16th international conference on World Wide Web WWW '07**

Publisher: ACM Press

Full text available: pdf(782.94 KB) Additional Information: full citation, abstract, references, index terms

Phishing is a significant problem involving fraudulent email and web sites that trick unsuspecting users into revealing private information. In this paper, we present the design, implementation, and evaluation of CANTINA, a novel, content-based approach to detecting phishing web sites, based on the TF-IDF information retrieval algorithm. We also discuss the design and evaluation of several heuristics we developed to reduce false positives. Our experiments show that CANTINA is good at detectin ...

Keywords: TF-IDF, anti-phishing, evaluation, phishing, toolbar

13 Session 2: Email feedback: a policy-based approach to overcoming false positives

Saket Kaushik, William Winsborough, Duminda Wijesekera, Paul Ammann
November 2005 **Proceedings of the 2005 ACM workshop on Formal methods in security engineering FMSE '05**

Publisher: ACM Press

Full text available: pdf(205.07 KB) Additional Information: full citation, abstract, references, index terms

Current email-control mechanisms, though highly effective, are pro-ne to dropping desirable messages. This can be attributed to their coarseness in filtering out undesirable messages from desirable ones. As a result policies to control undesirable messages are often overly permissive. To allow policies to be more restrictive, the transmission mechanism must be made aware of the ways to document a message so that it is acceptable downstream, thus giving the senders a chance of meeting those requi ...

Keywords: constraint logic programming, email/spam control, policy advertisement, policy feedback

14 Student papers: Managing phishing threats in an organization

Charles Ohaya
September 2006 **Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06**
Publisher: ACM Press
Full text available: pdf(104.70 KB) Additional Information: full citation, abstract, references, index terms

As more organizations do business on the Internet, phishers have become sophisticated with their social engineering techniques. With little effort, phishers target employees via electronic media such as email, websites, IRC and instant messaging, soliciting and capturing confidential information. The very high probability of stealing confidential information via these techniques instead of the traditional techniques (e.g. telephone), is very attractive to phishers and poses a serious threat t ...

Keywords: phishing, security

15 Enabling email confidentiality through the use of opportunistic encryption

Simson L. Garfinkel
May 2003 **Proceedings of the 2003 annual national conference on Digital government research dg.o '03**
Publisher: Digital Government Research Center
Full text available: pdf(51.35 KB) Additional Information: full citation, abstract, references

Software for encrypting email messages has been widely available for more than 15 years, but the email-using public has failed to adopt secure messaging. This failure can be explained through a combination of technical, community, and usability factors. This paper proposes a new approach to email security that employs opportunistic encryption and a security proxy to facilitate the opportunistic exchange of keys and encryption of electronic mail. While it appears that this approach offers less se ...

16 Short papers -- works in progress: Pvault: a client server system providing mobile access to personal data

Ravi Chandra Jammalamadaka, Sharad Mehrotra, Nalini Venkatasubramanian
November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press
Full text available: pdf(134.27 KB) Additional Information: full citation, abstract, references, index terms

In this paper we describe the design for the *Pvault* software, which is a personal data manager that stores and retrieves data from a remote untrusted data server securely. The major advantage of *Pvault* is that it allows users to access their personal data from any trusted remote computer. We will describe the issues and solutions for maintaining data confidentiality and integrity when the data is stored at the remote sever, since the server itself is untrusted. *Pvault* also p ...

Keywords: cryptography, database, encryption, mobile access, secure sharing, secure storage, security, untrusted service provider model

17 Inferring binary trust relationships in Web-based social networks

Jennifer Golbeck, James Hendler
November 2006 **ACM Transactions on Internet Technology (TOIT)**, Volume 6 Issue 4

Publisher: ACM Press
Full text available: pdf(1.36 MB) Additional Information: full citation, abstract, references, index terms

The growth of Web-based social networking and the properties of those networks have created great potential for producing intelligent software that integrates a user's social network and preferences. Our research looks particularly at assigning trust in Web-based social networks and investigates how trust information can be mined and integrated into applications. This article introduces a definition of trust suitable for use in Web-based social networks with a discussion of the properties that w ...

Keywords: Social networks, online communities, semantic Web, small worlds, trust

18 Content-triggered trust negotiation
Adam Hess, Jason Holt, Jared Jacobson, Kent E. Seamons
August 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 3
Publisher: ACM Press
Full text available: pdf(815.36 KB) Additional Information: full citation, abstract, references, citings, index terms

The focus of access control in client/server environments is on protecting sensitive server resources by determining whether or not a client is authorized to access those resources. The set of resources is usually static, and an access control policy associated with each resource specifies who is authorized to access the resource. In this article, we turn the traditional client/server access control model on its head and address how to protect the sensitive content that clients disclose to and r ...

Keywords: Trust negotiation, access control, authentication, credentials

19 Invited workshop on information technology and its applications: software development, disaster engineering, and security: Characteristics and responsibilities involved in a Phishing attack
Alta van der Merwe, Marianne Loock, Marek Dabrowski
January 2005 **Proceedings of the 4th international symposium on Information and communication technologies WISICT '05**
Publisher: Trinity College Dublin
Full text available: pdf(66.42 KB) Additional Information: full citation, abstract, references

'Phishing' is a fraudulent activity defined as the creation of a replica of an existing Web page to fool a user into submitting personal, financial, or password data. There are security service guidelines for both software security and web site security development environments. Developers use these guidelines when planning new systems (or during re-engineering of existing systems) to ensure a secure environment. The purpose of this paper is two-fold: firstly to consider the characteristics of a ...

20 Digital village: Malware month
Hal Berghel
December 2003 **Communications of the ACM**, Volume 46 Issue 12
Publisher: ACM Press
Full text available: pdf(101.12 KB) html(21.22 KB) Additional Information: full citation, abstract, index terms

August 2003: SoBig, W32/Blaster, and the malware month of the millennium.

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Results for "((spoof <in>metadata) <and> (email<in>metadata))"

e-mail

Your search matched **1** of **1618078** documents.

A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

((spoof <in>metadata) <and> (email<in>metadata)) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **PHONEY: mimicking user response to detect phishing attacks**
   Madhusudhanan Chandrasekaran; Ramkumar Chinchani; Shambhu Upadhyay
   World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006. In Symposium on a
   26-29 June 2006 Page(s):5 pp.
   Digital Object Identifier 10.1109/WOWMOM.2006.87
   AbstractPlus | Full Text: PDF(352 KB) IEEE CNF
   Rights and Permissions

Web Results **1 - 10** of about **295,000** for **spoof email sender address**. (**0.10** seconds)

Understanding **E-mail** Spoofing
However, the **sender** could write any name and **address** there; you have no assurance that the letter really is from that person and **address**. **E-mail** messages ...
www.windowsecurity.com/articles/**Email-Spoof**ing.html - 37k - Cached - Similar pages

Spoof Email Tutorial - Page 2
A. **Sender's Email Address Spoof email** may include a forged **email address** in the "From" line - Some may actually be real **email** addresses that have been ...
pages.ebay.com/education/**spoof**tutorial/**spoof**_2.html - 10k - Cached - Similar pages

DataStronghold.com - How to **Spoof** an **Email** Without Software
So many times I hear people asking how to **spoof** an **email sender address**. This is a relatively easy task but I find so many false advertisements for software ...
www.datastronghold.com/.../general-security-articles/how-to-**spoof**-an-**email**-without-software.html - 65k - Jul 20, 2007 - Cached - Similar pages

Are you the Klez monster? | CNET News.com
And it pairs this bogus **sender's address** with one of more than 120 different ... The Klez variant's ability to **spoof** the source of infected **e-mail** makes it ...
news.com.com/2100-1001-916945.html - 42k - Cached - Similar pages

email being rejected (**Sender address** rejected: not logged in ...
[Archive] **email** being rejected (**Sender address** rejected: not logged in) **Email**. ... one of those users on our system didn't **spoof** your **email address** then, ...
forum.powweb.com/archive/index.php/t-38402.html - 39k - Cached - Similar pages

"How can I recognize fake Paypal **email**?" from the Ask Dave Taylor ...
A fake **sender's address**. A **spoof email** may include a forged **email address** in the "From" field. This field is easily altered. A false sense of urgency. ...
www.askdavetaylor.com/how_can_i_recognize_fake_paypal_**email**.html - 30k - Cached - Similar pages

The latest Internet Explorer bug brings more **Spoof Email** and ...
Treat all **email** with suspicion - What you see in the **email** body can be forged, the **sender's address** or return **address** can be forged and the **email** header can ...
www.w3reports.com/index.php?itemid=118 - 23k - Cached - Similar pages

E-mail spoofing - Wikipedia, the free encyclopedia
E-mail spoofing is a term used to describe fraudulent **email** activity in which the **sender address** and other parts of the **email** header are altered to appear ...
en.wikipedia.org/wiki/E-mail_**spoof**ing - 17k - Cached - Similar pages

Processor Editorial Article - **Email** Authentication
First, the bad news: It's incredibly easy to **spoof email** systems, and unless you ... When spammers obey the protocol by not spoofing their **sender address**, ...
www.processor.com/editorial/article.asp?article=articles/P2648/30p48/30p48.asp&guid= -

26k - Cached - Similar pages

Email Reaction_spoof emails
The current problem with **spoof email** stems from how it is sent. ... SMTP receivers verify the **sender address** against this information, and can distinguish ...
www2.**email**reaction.com/**Email**Reaction_**spoofemail**s.asp - 23k - Cached - Similar pages

1 2 3 4 5 6 7 8 9 10 **Next**

---

spoof email sender address Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---